

REMARKS

This Application has been carefully reviewed in light of the *Office Action*. At the time of the *Office Action*, Claims 1-34 were pending and rejected. Applicant has amended Claims 1, 9, and 16, and canceled Claims 27-29. Applicant respectfully requests reconsideration and favorable action in this case.

Claim Objections

The Examiner objects to Claims 9 and 28 as allegedly being indefinite for including the phrase “operable to.” Solely to advance prosecution and without conceding to the propriety of the objection, Applicant has amended Claims 9 and 28 to recite “configured to.” Applicant thanks the Examiner for his suggestion.

Rejections Under 35 U.S.C. § 101

The Examiner rejected Claims 9-15, 25, 28 and 31 under 35 U.S.C. § 101 as allegedly being directed to software *per se*. While Applicant does not necessarily agree with the propriety of this rejection, and solely to advance prosecution, Applicant has amended Claim 9 to recite a *tangible* processor controlled device. Accordingly, Applicant respectfully requests the Examiner to withdraw the rejections of Claims 9-15, 25, 28 and 31 under 35 U.S.C. § 101.

Rejections Under 35 U.S.C. § 102 and §103

The Examiner rejected Claims 1-5, 9-11, 15-20, 24-32 and 34 under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Publication No. 2003/0061515 to Kindberg et al. (“*Kindberg*”). The Examiner rejected Claims 6-8, 12-14, and 21-23 under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Kindberg* in view of U.S. Patent No. 7,080,000 to Cambridge (“*Cambridge*”). The Examiner further rejected Claim 33 under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Kindberg* in view of U.S. Patent No. 6,968,394 to El-Rafie (“*El-Rafie*”). Applicant respectfully traverses those rejections for the reasons stated below.

I. *Kindberg* fails to disclose the limitations of amended Claim 1.

Claim 1, which has been amended to include limitations formerly recited in dependent Claim 27, now recites (emphasis added):

A method for maintaining computer security . . . wherein . . . comparing the received incoming message with the signature file to determine whether the incoming message is malicious comprises **determining whether the incoming message is malicious by comparing a length of a URL in a message header of the incoming message with the predefined length in the signature file.**

In the *Office Action*, the Examiner rejected those limitations with respect to Claim 27 by relying on *Kindberg*. See *Office Action*, page 7. *Kindberg*, however, discloses “[a] mechanism for providing a user with selective access to resources on an intranet” See *Kindberg*, Abstract. As explained by *Kindberg*, “[c]apabilities are used to represent URLs of resources within the domain 200. In order to use a capability, a client 203 must present the capability to a reverse proxy server 201 running on the firewall of the domain 200 . . . Upon receiving a capability-enabled URL, the reverse proxy server verifies its authenticity and then issues a request to the intranet web server 202 which manages the resource.” See *Kindberg*, paragraphs [0035] - [0037].

In particular, the Examiner relied on a capability recognition procedure described in paragraph [0052] of *Kindberg* to reject the above-quoted limitations of Claim 1. *Office Action*, page 7. However, *Kindberg*’s capability recognition procedure does not allow for determination of whether a request is malicious. According to paragraph [0052]:

In step 600, the reverse proxy server 201 receives a capability-enabled URL. The capability character string **may be recognized** as such by referring to the table used to track issued capabilities and avoid capability/URL ambiguity. Alternatively, all URLs having a character string conforming to the length and composition conforming to the established capability format (allowing for escape sequences if present) may be passed to step 605.

Kindberg, paragraph [0052] (emphasis added). That is, the passage merely discloses that a URL may be recognized as being capability-enabled (but not recognized as malicious) if its character string conforms to the established capability format (i.e., in length and composition). Consequently, paragraph [0052] of *Kindberg* fails to disclose, teach, or suggest “determining whether the incoming message is malicious by comparing a length of a URL in a message header of the incoming message with the predefined length in the signature file” as recited in Claim 1.

The Examiner also relies on paragraphs [0058] and [0059] of *Kindberg* to teach the above-quoted limitations of Claim 1. *Office Action*, page 7. However, those paragraphs

merely disclose that rules may be established to govern the types of CGI script that may be invoked using a capability. According to paragraph [0059]:

Secure web exporting allows the specification of rules regarding the type and content of arguments for a CGI script invoked through a capability. **It is possible to list the acceptable arguments, or explicitly exclude certain arguments, and add to or replace values for arguments which the user has specified in the request.**

Kindberg, paragraph [0059] (emphasis added). That is, the passage merely discloses that various arguments in a request may be excluded, deemed acceptable, or modified (e.g., by adding or replacing values) using rules governing the type and content of arguments for a CGI script invoked through a capability. However, the passage is completely devoid of any teaching of “determining whether the incoming message is malicious by comparing a length of a URL in a message header of the incoming message with the predefined length in the signature file” as recited in Claim 1.

The Examiner also relies on a capability verification procedure described in paragraph [0054] of *Kindberg* to reject limitations similar to those of Claim 1, but recited in Claim 34. See *Office Action*, page 11. However, *Kindberg*’s capability verification procedure does not allow determination of whether a request is malicious. *Office Action*, page 4. According to paragraph [0054]:

In step 610, **the capability is verified** by first determining whether the resolved identification number corresponds to a database record. If a database record exists for the identification number, the decoded expected random number is checked for a match with the random number in the identified database record. If a record exists for the decoded identification number and the random number in the record matches the expected random number, then **the capability is accepted as genuine**. If either the identification number or random number does not match, the request is rejected and can either be ignored or responded to with an error message.

Kindberg, paragraph [0054] (emphasis added). That is, the passage merely discloses that a capability-enabled URL is matched with a database record to determine whether the capability-enabled URL is genuine and that the capability-enabled URL is ignored based on whether it is determined to be genuine, but not on whether it is determined to be malicious. Consequently, paragraph [0054] of *Kindberg* fails to disclose, teach, or suggest “determining whether the incoming message is malicious by comparing a length of a URL in a message

header of the incoming message with the predefined length in the signature file" as recited in Claim 1.

For at least these reasons, independent Claim 1 and its dependent claims are allowable under 35 U.S.C. § 102 and 35 U.S.C. § 103. For analogous reasons, independent Claims 9, 16, and 34 and their respective dependent claims are allowable under 35 U.S.C. § 102 and 35 U.S.C. § 103.

II. All Claims are in condition for allowance.

For at least the reasons stated above, Applicant respectfully contends that each and every claim is in condition for allowance. Moreover, Applicant respectfully contends that none of the deficiencies described above with respect to *Kindberg* are accounted for by any of the remaining references cited by the Examiner or by the knowledge of one of ordinary skill in the art.

No Waiver

Additionally, Applicant has merely discussed example distinctions from the references cited by the Examiner. Other distinctions may exist, and Applicant reserves the right to discuss these additional distinctions in a later Response or on Appeal, if appropriate. By not responding to additional statements made by the Examiner, Applicant does not acquiesce to the Examiner's additional statements, nor does Applicant necessarily concede to the veracity of any characterization of Applicant's claims or the prior art references made by the Examiner. The example distinctions discussed by Applicant are sufficient to overcome the Examiner's rejections.

CONCLUSION

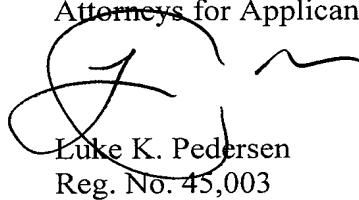
Applicant has made an earnest attempt to place this case in condition for allowance. For at least the foregoing reasons, Applicant respectfully requests full allowance of all pending claims.

If the Examiner feels that a telephone conference would advance prosecution of this Application in any manner, the Examiner is invited to contact the undersigned Attorney for Applicant, at the Examiner's convenience at (214) 953-6655.

No additional fee is believed to be due at this time. However, the Commissioner is hereby authorized to charge any additional fees or credit any overpayment to Deposit Account No. 02-0384 of BAKER BOTTS L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant



Luke K. Pedersen
Reg. No. 45,003

Date: May 4, 2009

CORRESPONDENCE ADDRESS:

Customer No. **05073**